opentext™

Smarter cybersecurity for Energy

Defend against the most sophisticated cyberattacks on energy infrastructure

"Cybersecurity incidents targeting energy and commodities infrastructure reached record highs in 2022."

– S&P Global [1]

Industry backdrop

The pressure is on Energy corporations to advance cybersecurity measures, as increasingly sophisticated cyberthreats are putting organizations at risk and can lead to unplanned asset downtime or hazardous events, threatening the safety of employees, surrounding communities, or the environment.

Oil assets and infrastructure continue to be a major target for hackers, accounting for a third of all incidents since 2017, followed by electricity networks, which make up a quarter of all incidents.[2] Examples of notable cyberattacks around the globe include:

- A large-scale ransomware attack that disrupted operations at oil terminals in Germany, before spreading to other terminals in Europe—the third largest global consumer of oil.
- A $50-million cyber extortion of Saudi Aramco, the world's largest oil exporter and third largest oil producer.
- A six-day shutdown at Colonial Pipeline, which transports 45 percent of the fuel to the United States' East Coast, stopping the transport of 2.5 million barrels of refined oil product per day (a value of $225 million per day at today's prices).

With the average cost of a data breach in the Energy sector reaching $4.7 million[3] —a record high—the economic risk has never been greater. However, this hefty cost will pale in comparison if the assertion by former US Secretary of Defense, Leon Panetta, holds true: "The next Pearl Harbor we confront could very well be a cyberattack that cripples our power systems, our grid, our security systems, our financial systems, our governmental systems."[4]

In addition, Energy companies must adhere to new regulations, such as The European Parliament's NIS2 (Network Information Security) Directive and the United States' Executive Order 13800 Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.

This paper explores how Energy companies can deploy smarter cybersecurity protection to gain 360-degree visibility across the organization to reduce business and operational risk, minimize downtime, and maintain privacy and compliance.

OpenText vision: Smarter cybersecurity for Energy

Gaps in cybersecurity governance can lead to delayed projects, unplanned asset downtime, outages and elevated operational risk from multiple attack vectors, insider threats, or attacks via supply chain tampering.

Smarter cybersecurity can help Energy corporations protect valuable and sensitive information and gain 360-degree visibility across endpoints and network traffic to ensure energy is always flowing safely and securely.

Smart oilfields, smart grids, smart refineries, and other smart asset initiatives are only "smart" if they don't get hacked. These initiatives have predominantly focused on sophisticated operational technology, with cybersecurity initiatives kept separate. With the convergence of information technology and operational technology systems, smart energy asset initiatives have room to get smarter by employing cybersecurity best practices and technologies across the two systems.

[1] S&P Global, Cyberattacks surge in 2022 as hackers target commodities. (October 2022)

[2] Power & Beyond, More cyber attacks in 2022 than ever before. (March 2023)

[3] IEA.org, Cybersecurity—is the power system lagging behind? (July 2021)

[4] Financial Times, US Power Plants Vulnerable to Attack, (2011)

If any of the following ring true, there are opportunities for cybersecurity improvements:

- Common vulnerabilities and exposures (CVEs) are not detected.
- Costly “all hands on deck” scenarios are needed to close security gaps.
- Alarm trends aren’t being reduced.
- The total cost of ownership (TCO) for cybersecurity investments is high due to vendor sprawl.
- Supply chains aren’t confidently secured.
- Artificial intelligence isn’t being used to protect the organization.

Smarter cybersecurity allows organizations to respond to an evolving threat landscape, adapting to the ever-expanding attack surface across energy infrastructure, as well as responding to challenges posed by a multi-platform, multi-cloud environment. With a focus on data sovereignty and privacy, this approach safeguards the integrity of sensitive information.

As data flow grows exponentially, smarter cybersecurity efficiently protects information in transit. Smarter cybersecurity also embraces volatility and resilience, ensuring systems can withstand pervasive disruptions and geopolitical risk.

> “**Even the most secure organizations will experience a breach at some point.** But what separates us now is how quickly we can detect a genuine threat and respond, because the longer a threat remains hidden, the more damage it does. With OpenText ArcSight, we don’t just detect real attacks quickly, but we also automate orchestrated responses in near-real time.”
>
> – Dmitriy Ryzhkov, Senior Information Security Analyst, NPC Ukrenergo

Using information management to defend against energy infrastructure cyberattacks

The statement, “It isn’t a matter of if you get hacked, but when” has never been more accurate, especially for the Energy industry. Quite simply, hacks occur because energy data is valuable. By encrypting sensitive and proprietary data at rest, organizations can prevent unauthorized access. A modern and integrated cybersecurity framework can enable organizations to protect data from a broad range of cyberattacks, such as client-side, supply chain, business app, and automated attacks.

The National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF) provides a foundation for which companies, regardless of industry, can structure a comprehensive cybersecurity program. Critical cybersecurity components used across the Energy sector to develop a comprehensive cybersecurity program include: Network Security, Identify and Access Management (IAM), Data Protection, Application Security, Endpoint Security, Vulnerability Management, Threat Protection, Risk and Compliance, and Forensics and Insider Risk.[5] OpenText cybersecurity solutions address all nine of these components to protect Energy corporations and their infrastructure.

By using a leading cybersecurity platform, Energy companies can confidently protect sensitive information and securely automate information flow inside, outside, and across the enterprise so that team members can work smarter. The result is improved information protection and lower operational risk. OpenText helps organizations boost security and trust in multiple ways, enabling:

Smarter cyber resilience

OpenText cybersecurity solutions improve organizations' security posture with capabilities such as: threat detection and response, application security, identity and access management, data protection and privacy. A portfolio of complementary security capabilities provides 360-degree visibility across endpoints and network traffic to identify, triage, and investigate anomalous and malicious behavior.

OpenText also offers cloud-based global signal analytics technology that discovers malicious traffic, defines digital genealogies, and defends against future attacks. It bolsters resilient defenses with insights derived from internet traffic, indicating the intent of activity in the network.

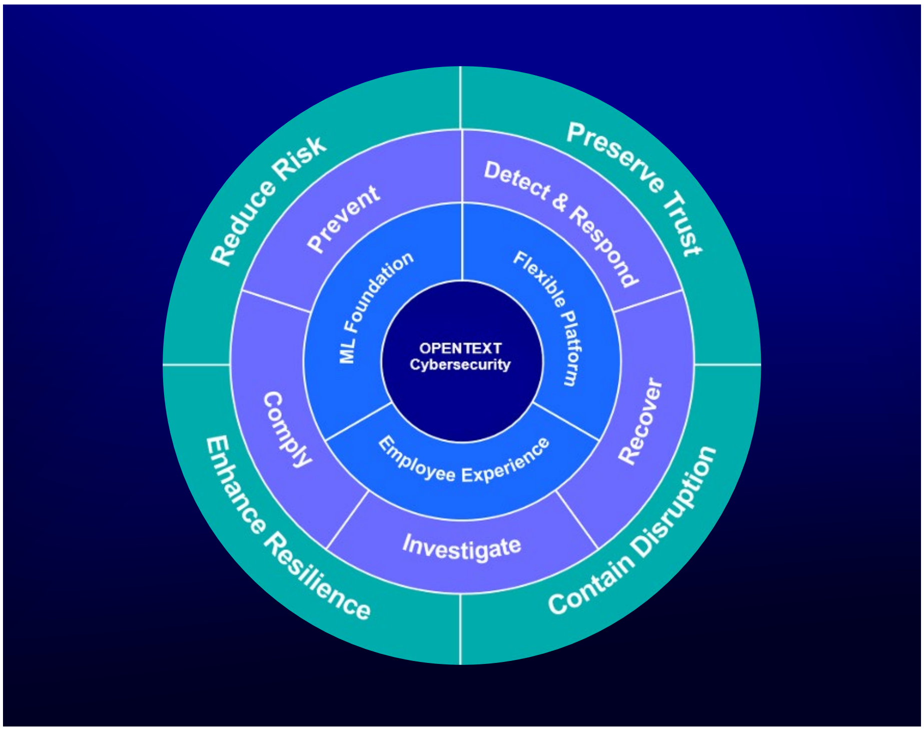

Figure 1. Helping companies simplify security

[5] Natural Gas Council, Defense-In-Depth: Cybersecurity in the Natural Gas & Oil Industry

Improved IT efficiency and performance

OpenText IT Operations Management capabilities encompass a comprehensive suite of tools that optimize, monitor, and manage an organization's IT infrastructure. The platform offers end-to-end visibility into system performance, helping Energy corporations identify and address issues before they impact operations. The platform includes vulnerability risk management and vulnerability management, ensuring that potential weaknesses are quickly identified and remedied. It also facilitates configuration and OS compliance management and guarantees that systems adhere to security and operational standards.

The platform streamlines automated server provision and lifecycle management, ehancing efficiency and resource utilization. Furthermore, it offers cloud-ready scalability and flexibility, empowering organizations to adapt to the ever-changing IT landscape while maintaining the reliability, security, and scalability of their IT environment.

> "By taking a different approach to visualizing our risk themes, embracing modern, business-enabling technologies, such as ArcSight, and establishing an advanced security operations center (SOC), **we have experienced a 30-percent reduction in alarms**, ensuring our resources are directed most effectively."
>
> – Jacob Jacob, Specialist Cybersecurity, Dubai Electricity and Water Authority

Advanced threat detection and prediction

Despite the global Energy sector producing the most energy on record for any given year, the industry will never move this slowly again. This also holds true for threat detection across energy infrastructure. Artificial intelligence, analytics and Internet of Things are key technologies for accelerating asset operations and project execution and mitigating cybersecurity risk.

OpenTextTM Aviator Platform is a family of practical and trusted generative AI capabilities that combine new threat detection approaches with machine learning models. AI-based cybersecurity not only automates the detection and response to new threats but also enables behavioral threat hunting.

Why OpenText

The OpenText Cybersecurity Platform protects more than 800,000 businesses of all sizes across 180 countries. More than 78 million end users are protected by one or more cybersecurity solutions within our full-stack cybersecurity platform.

OpenText is also the world's leader in the information management domain. We serve thousands of energy companies across the world to organize, integrate, protect, and automate data as it flows inside and outside the organization. No information management platform is more secure or scalable to manage high volumes of information at various stages of the asset lifecycle.

We welcome the opportunity to be a strategic partner in your cybersecurity journey to help you take your smart assets and operations from smart to smarter with OpenText.

Proposed next steps

Together, let's outline a vision and identify opportunities to quickly improve your cybersecurity key performance indicators. Below are suggested next steps to ensure your cybersecurity journey is in lock step with your information management journey.

- Introductory meeting: Bring together your OpenText Global Account Director or Senior Account Representative with your organization's Account Business Unit CISO, VP of Security Operations, VP of Emergency Operations & Incident Management, VP of Security Engineering & Asset Security, and/or other security and risk management positions.
- Joint roadmap exchange: A one-half to full-day information exchange with your information security and risk management leaders and OpenText to learn more about your cybersecurity initiatives, current approaches and obstacles, and provide an overview of best practices and cybersecurity solutions to support those initiatives.
- Business Value Consulting workshop: The OpenText Business Value Consulting team will engage with information security teams to assess the current state of information security business processes and quantify the business impact of OpenText cybersecurity solutions.